Procedure for increasing the manipulation security for a bi-directional contactless data transmission

BACKGROUND

Field of the invention

The subject invention concerns a procedure for increasing the manipulation security for a bi-directional contactless data transmission by means of a first transmission and receiver unit (BA) and a second transmission and receiver unit.

Description of the related technology

Systems for bi-directional contactless data transmission are preferably used for identification systems. These consist of a transponder, which is either integrated in a key fob or a so-called Smart card, and a stationary base unit. In vehicle engineering – one of the principal areas of application for transponder technology, the base unit is fitted into vehicles. The communication between transponder and base unit is based on an inductive coupling, with generally either the unidirectional or the bi-directional protocol being used for communication between transponder and base unit. The complete identification process for the transponder or base units is designated as authentication. If the transponder does not have its own power supply, or if this is empty, it will obtain its energy from the LF field emitted by the base unit. In these cases, the data transmission range will be restricted to just a few centimeters. In other cases, the range is determined by security requirements and system limitations. Inasmuch as a particularly high level of security is demanded with regard to identification - for example when obtaining so-called "passive entry", i.e. when opening the vehicle by pulling on the door handle, - the communication distance will be limited to 2.5 m when using the bi-directional protocol. To this end, preferably a LF carrier frequency of 125 kHz is used for the communication between motor vehicle and key, whilst for the communication from key to motor vehicle a carrier frequency is used which is preferably within the UHF range of 433.92 MHz. In the

case of reduced security requirements, such as e.g. for active opening by pressing the key switch when being in the vicinity of the motor car, a range of up to 30 m is permitted. To this end, the unidirectional protocol will generally be used in connection with a UHF carrier frequency near 433.92 MHz. The greater security of the bi-directional protocol during the authentication process is that in comparison to the unidirectional protocol – which only provides for a single authorization check of the transponder – the base unit will also be authenticated. For all applications in transponder technology, it is important that the time required for the authentication process is kept as short as possible. In particular in motor vehicle engineering, the entire time period taken for authentication should not exceed 130ms. Due to the high security requirements, a bi-directional protocol is used as a matter of preference. In order to further increase manipulation security, in particular for the bi-directional protocol, new solutions are being searched for.

With the present state of the art, as described for instance in VDI Report No. 1415, 1998, an authentication with a bi-directional protocol will be effected according to the following pattern:

As soon as the transponder has been activated by means of an activation command sent out by a base unit, e.g. by operating the door handle on the motor vehicle, an authentication can be effected by means of a mutual identification check. To this end, random numbers – so-called "Challenges" - will be exchanged, from which, in the transponder as well as in the base unit, a permanently programmed algorithm will calculate numbers that are designated as a response. Then the calculated response between transponder and base unit will be replaced again and checked for agreement with the user calculated response. If these checks are positive for the transponder as well as the base units, authentication is successful. The data sequences exchanged for identification will be modulated onto the UHF carrier frequency. The carrier frequency will be generated by means of a quartz. The precision of the latter will typically be ±100ppm; relative to the carrier frequency of 433.92 MHz, this corresponds to a precision of ±43.392 KHz. As both the transponder as well as the base unit operate with their own frequency stabilization, and as even the respective

exciter circuits for the quartzes feature a frequency imprecision, the input bandwidth in the respective receiver unit is designed for approximately 300-600 kHz in order to ensure stable communications.

Due to the significant bandwidth of the input filters, however, it is possible to provide for an additional extension of the communication distance between transponder and base unit, using suitable aids, without any interference in the authentication process for a bi-directional protocol. But as the extension allows distances to be bridged that are significantly greater than 2.5 m, a manipulation cannot be excluded either. To this end, the signals emitted from the base unit and the transponder will be forwarded by means of two trade standard repeaters, such that one repeater will be located in the vicinity of the base unit whilst the other repeater is located in the vicinity of the transponder. In order to avoid feedback, both repeaters mix the signals emitted at e.g. 433.92 MHz onto another frequency band. The minor frequency shift which occurs will not be noticeable due to the relatively wide input filters. Depending on the transmission power of the repeater, great distances can be bridged in this way in order to obtain within the shortest possible time (130ms) quite unnoticed unauthorized access – to a motor vehicle, for instance. In order to close this significant security gap during authentication on the basis of a bi-directional data transmission, solutions need to be found by means of which any unintended extension of the communication distance will be detected.

Summary of the invention

It is the task of the invention described here to state a low cost procedure which, for a bi-directional contactless data transmission, makes any unintended extension of the communication distance between the base unit and the transponder significantly more difficult, and thus offers significantly increased security against manipulation. However, this should not lead to any increase in total authentication time.

In accordance with the invention, this task is solved by a procedure of the type described above, featuring the characteristics of Patent Claim 1. Favorable implementations are the subject of sub-claims.

Investigations carried out by the applicant have shown that the manipulation security of the transponder base unit system can be increased significantly, if, in the case of a bi-directional communication between transponder and base unit, the value of at least one of the physical quantities from the electromagnetic signals used for information exchange purposes is changed reversibly. To this end, an electromagnetic signal will be emitted from a transmitter unit, for instance the transmitter unit included in the base unit. For this electromagnetic signal which is then received by the transponder, the value of one of the physical quantities characterizing the signal will then be changed; and then the changed electromagnetic signal will be returned to the base unit. In the base unit, this value will subsequently be changed back. By means of a comparison, i.e. comparing the reversibly changed value of the physical quantity with its original value, it will then be possible to check whether the deviation of this physical quantity is within an expected tolerance range. With regard to the existing authentication process according to the bi-directional protocol, which only contains a comparison of numeric values (response) calculated from random numbers, the additional comparison of values allows any non-permissible extension of the communication distance between transponder and base unit to be detected. The precision of the procedure is proportionate to the size of the time window which is used for the comparison of the reversibly changed value with the original value of the physical quantity.

According to a first embodiment it has been found to be particularly advantageous if, as a physical quantity whose value is changed reversibly, the frequency of the electromagnetic waves is used. This is implemented by generating a UHF carrier frequency – at 433.92 MHz for instance – in the base unit and transmitting the same to the transponder. Additionally, a data signal can be modulated onto this carrier frequency. In the transponder, the data signal will then be separated for further

evaluation and, finally, the received UHF carrier frequency will be converted to a different frequency range. Following the possible modulation with a data signal, the changed carrier frequency will be retransmitted to the base unit. In the base unit, after re-conversion to the original carrier frequency, a frequency comparison with the previously emitted carrier frequency will be effected. If, within the time window under consideration, the frequency shift determined in this way is smaller than a preset value, an unauthorized extension of the communication distance can be excluded. Depending on the application, this check can be effected either in parallel or in series to the calculation of the response numbers from the exchanged random numbers (challenge). The authentication of the transponder and base unit system will only be positive if the results of all individual checks are positive. In this connection, it has been found that the entire authentication process should be completed within 300ms at most.

Brief description of the figures

In the following, the invention will be illustrated and elucidated in accordance with a drawing. The figure shows:

Fig. 1 An embodiment of the invention as a procedure for checking a fixed frequency relationship in the case of a bi-directional data transmission.

Description of the preferred embodiments

Figure 1 shows an embodiment of the procedure in accordance with the invention. As shown here, in the base unit, the carrier frequency fUL generated by an oscillator OSC will be modulated by the transmitter TX1 with a data signal. The signal fULmod generated in this way will be emitted by a transmitter unit. In the transponder, the frequency f'UL is generated from the received signal f'ULmod by means of the frequency regeneration unit CLK2. Together with the signal f'UL generated in this way, and the input signal f'ULmod, the data signal modulated onto the carrier frequency will be regained in the receiver RX2. From the frequency f'UL the frequency f'DL is generated, using the synthesizer Synth2, by multiplying the

frequency f'UL with the number Z. Investigations of the applicant have shown that it is particularly advantageous if the number Z is built up from a ratio of two natural numbers. In the transmitter TX2, the transmission data will be modulated on, followed by the generation and emission of the signal f'DLmod from the frequency f'DL. In the base unit, the transponder data are regained from the received signal f''DLmod by means of the receiver unit RX1. To this end, the receiver unit RX1 will be fed with the frequency fDL generated, using the synthesizer Synth1, from the frequency fUL by means of multiplication with the number Z. Furthermore, the frequency f''DL is generated from the received signal f''DLmod by means of the frequency regeneration unit CLK1. Using the synthesizer Synth3, the frequency f''UL is generated from the frequency f''DL by dividing the same by the number Z. Using the signal processor SP, the difference of the two frequencies fUL and f''UL is calculated and compared with a preset limit value over a time period t. If the difference of the two frequencies fUL and f''UL is below the preset limit value, an unauthorized extension of the communication distance between the transponder and the base unit can be excluded. Starting from a time window of e.g. 20ms, it is thus possible to detect reliably frequency shifts of 1ppm; at 433.92 MHz this shift is 433 Hz. This value is thus smaller by a factor 100 than the value provided by the previous state of the art.

Other than in the embodiment of the procedure according to this invention shown in Figure 1, where the authentication has been effected respectively by a transponder and a base unit each, the procedure can also be used for authentication in the case of several transponders or base units. In the same way, a transponder may be selected as a starting point for the emission of an electromagnetic signal.